Los Teoremas de Incompletitud de Gödel: Parte I: Cálculo de Predicados

Guillermo Morales Luna

Departmento de Computación
CINVESTAV-IPN

gmorales@cs.cinvestav.mx

2-o Encuentro Nacional de Epistemología y Matemáticas, Zacatecas

In Memoriam Guillermo Moreno

Contenido

Contenido

Cálculo de predicados: Sintaxis

Definición

Un alfabeto L propio para una teoría de primer orden es la unión de:

Símbolos especiales $SE = \{(,)\}$

Conectivos lógicos $CL = \{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$

Cuantificadores $Q = \{\forall, \exists\}$.

$\forall$: *"para todo", es el cuantificador universal y*

$\exists$: *"existe", es el cuantificador existencial.*

Variables $Var = \{x_0, x_1, x_2, \ldots\}$

Símbolos constantes $Cte = \{c_0, c_1, c_2, \ldots\}$

Símbolos de relaciones $Rel = \left\{R_j^i\right\}_{j\geq 0}^{i\geq 1}$.

Símbolos de funciones $Fun = \left\{f_j^i\right\}_{j\geq 0}^{i\geq 1}$.

Los conjuntos de constantes, de relaciones y de funciones han de ser finitos.

Su unión $Sig = Cte \cup Rel \cup Fun$ es la signatura de la teoría.

Los superíndices i en los símbolos de relación o de función denotan a su respectiva aridad: el número de argumentos o de plazas que involucran.

Sea L_{CA} el alfabeto cuya signatura es la unión de los conjuntos siguientes:

Cte:

0	unidad aditiva
1	unidad multiplicativa

Rel:

$R_0^2(x,y) := [x = y]$ igualdad usual entre elementos

Fun:

$f_0^1(x) := [-x]$	inverso aditivo
$f_1^1(x) := [x^{-1}]$	inverso multiplicativo
$f_0^2(x,y) := [x + y]$	adición
$f_1^2(x,y) := [x \cdot y]$	multiplicación

Algebras booleanas

Sea L_{AB} el alfabeto cuya signatura es la unión de los conjuntos siguientes:

Cte:

0	elemento mínimo
1	elemento máximo

Rel:

$R_0^1(x) := [Atomo(x)]$	x es un átomo
$R_0^2(x,y) := [x = y]$	igualdad usual entre elementos
$R_1^2(x,y) := [x \leq y]$	menor o igual a
$R_2^2(x,y) := [x \geq y]$	mayor o igual a
$R_3^2(x,y) := [x < y]$	menor que
$R_4^2(x,y) := [x > y]$	mayor que
$R_5^2(x,y) := [x?y]$	x e y no son comparables

Fun:

$f_0^1(x) := [\overline{x}]$	complemento
$f_0^2(x,y) := [x \wedge y]$	ínfimo de dos elementos
$f_1^2(x,y) := [x \vee y]$	supremo de dos elementos

Teoría de conjuntos

Sea L_{TC} el alfabeto cuya signatura es la unión de los conjuntos siguientes:

Cte:

$\emptyset$ conjunto vacío

Rel:

$R_0^2(x,y) := [x \in y]$ pertenencia
$R_1^2(x,y) := [x \subset y]$ inclusión
$R_2^2(x,y) := [x = y]$ igualdad

Fun:

$f_0^1(x) := [x^c]$ complemento
$f_1^1(x) := [\mathcal{P}(x)]$ conjunto de partes
$f_0^2(x,y) := [x \cup y]$ unión
$f_1^2(x,y) := [x \cap y]$ intersección

Parentesco

Sea L_{Pco} el alfabeto cuya signatura consta de los símbolos de relación y de función siguientes:

Rel: Hay símbolos unarios y binarios, cada uno con una connotación obvia:

- Unarios: varón, mujer, hijo_legítimo, bastardo. Cada uno de éstos es de la forma $p(x)$: "x es p".
- Binarios: Cada uno de los siguientes es de la forma $p(x, y)$: "x es p de y". Estos son: progenitor, hijo, hermano, tío, sobrino, primo, abuelo, nieto, bisabuelo, bisnieto, tatarabuelo, tataranieto, ancestro, descendiente, casamiento, cónyuge, concubino, suegro, yerno, nuera, cuñado, consuegro, concuño, padrastro, hijastro.

Fun: Igualmente, hay símbolos unarios y binarios, cada uno con una connotación obvia:

- Unarios: `padre`, `madre`, `marido`, `esposa`, `primogénito`, `abuelo_paterno`, `abuela_paterna`, `abuelo_materno`, `abuela_paterna`. Cada uno de éstos es de la forma $f(x)$: "el (la) f de x".
- Binarios: Cada uno de los siguientes es de la forma $f(x, y)$: "el (la) f de x y de y". Estos son: `hijo_mayor`, `hijo_menor`.

Sea pues $L = SL \cup Sig$ un alfabeto para una teoría de primer orden, y sea L^* el diccionario, es decir, el conjunto de palabras de longitud finita, con símbolos en L. En L^* distinguiremos a los conjuntos de términos y de fórmulas bien formadas.

Definición

El conjunto de términos, $Term(L)$ se construye recursivamente como sigue:

- *Las variables y las constantes son términos.*
- *Las funciones aplicadas sobre términos producen nuevos términos.*

Puesto en símbolos:

$$\begin{array}{rcl} x \in Var & \Rightarrow & x \in Term(L) \\ c \in Cte & \Rightarrow & c \in Term(L) \\ f^i_j \in Fun\ ,\ \xi_1, \ldots, \xi_i \in Term(L) & \Rightarrow & f^i_j\,(\xi_1, \ldots, \xi_i) \in Term(L) \end{array}$$

En el alfabeto L_{CA} de campos algebraicos:.

$$
\begin{array}{ll}
f_0^2\left(f_0^2\left(f_1^2\left(x_1, f_1^2\left(x_2, x_2\right)\right), f_1^2\left(x_3, x_2\right)\right), f_0^1\left(x_4\right)\right) & : x_1 x_2^2 + x_3 x_1 - x_4 \\
f_1^2\left(f_0^2\left(f_1^2\left(x_0, x_0\right), f_0^1\left(1\right)\right), f_0^2\left(f_1^2\left(x_0, x_0\right), f_0^1\left(1\right)\right)\right) & : (x_0^2 - 1)^2 \\
f_1^1\left(f_0^2\left(1, f_0^1\left(f_1^2\left(x_0, x_0\right)\right)\right)\right) & : \frac{1}{1-x_0^2}
\end{array}
$$

En el alfabeto de parentesco L_{Pco},

$\underline{\texttt{hijo\_mayor}}(\underline{\texttt{padre}}(x))$: el “hermano mayor” de x,

$\underline{\texttt{madre}}(\underline{\texttt{hijo\_mayor}}(x))$: acaso la “primera mujer” de x, e

$\underline{\texttt{hijo\_mayor}}(\underline{\texttt{abuelo\_paterno}}(x), \underline{\texttt{abuela\_paterna}}(x))$: tío mayor de x.

Fórmulas atómicas

Definición

Las *fórmulas atómicas*, *o* *átomos* *simplemente, se obtienen de evaluar símbolos de relación sobre términos:*

$$R^i_j \in Rel\ ,\ \xi_1, \dots, \xi_i \in Term(L) \quad \Rightarrow \quad R^i_j\left(\xi_1, \dots, \xi_i\right) \in Atom(L).$$

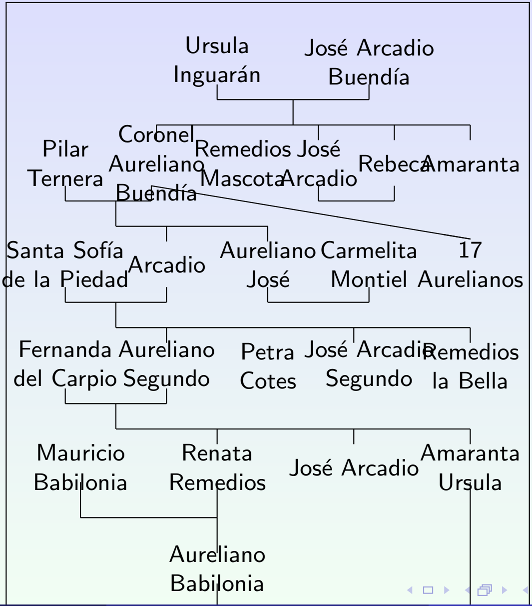
Por ejemplo, en el alfabeto L_{CA} de campos algebraicos, el átomo

$$R^2_0\left(f^2_0\left(f^2_0\left(f^2_1\left(x_1, f^2_1\left(x_0, x_0\right)\right), f^2_1\left(x_2, x_0\right)\right), x_3\right), 0\right)$$

representa la ecuación de segundo grado:

$$x_1 x_0^2 + x_2 x_0 + x_3 = 0.$$

Una estirpe condenada a cien años de soledad



Fórmulas bien formadas

Definición

El conjunto de fórmulas bien formadas, $Fbf(L)$ se obtiene partiendo de los átomos, componiéndolos con los conectivos lógicos y cuantificando adecuadamente sobre variables: Puesto en símbolos:

$$
\begin{array}{rcl}
R^i_j\,(\xi_1,\ldots,\xi_i) \in Atom(L) & \Rightarrow & R^i_j\,(\xi_1,\ldots,\xi_i) \in Fbf(L) \\
\phi \in Fbf(L) & \Rightarrow & \neg\phi \in Fbf(L) \\
\phi,\psi \in Fbf(L) & \Rightarrow & \phi\wedge\psi, \phi\vee\psi, \phi\rightarrow\psi, \phi\leftrightarrow\psi \in Fbf(L) \\
x \in Var(L),\ \phi \in Fbf(L) & \Rightarrow & \forall x\ \phi\,,\ \exists x\ \phi \in Fbf(L)
\end{array}
$$

Definición

Una variable $x \in Var$ aparece en un término $t \in Term(L)$ en una de las dos siguientes condiciones:

1. $t = x$
2. $t = f_j^i(t_1, \ldots, t_i)$ *y x aparece en algún t_{i_0}, con $i_0 \leq i$.*

Un término en el que no aparezcan variables se dice ser cerrado.

Definición

Las apariciones de variables en fórmulas se caracterizan como sigue:

1. *$x \in Var$ aparece libre en $R_j^i(t_1, \ldots, t_i)$ si x aparece en un t_{i_0}, $i_0 \leq i$.*
2. *$x \in Var$ aparece libre o ligada en $\neg\phi$, o $\phi * \psi$, con $* = \vee, \wedge, \rightarrow, \leftrightarrow$, si x aparece, libre o ligada respectivamente, en una de ϕ o ψ.*
3. *Si $x \in Var$ aparece libre en $\phi(x)$ entonces aparecerá ligada en $\forall x\, \phi(x)$ y en $\exists x\, \phi(x)$. Se dice que $\phi(x)$ es el alcance de x en $\forall x\, \phi(x)$ y en $\exists x\, \phi(x)$. Si y es una variable distinta de x entonces x aparecerá en $\forall y\, \phi(y)$ y en $\exists y\, \phi(y)$ igual que como aparece en $\phi(y)$.*

Las fórmulas que no contienen variables libres son llamadas enunciados.

Reglas de buena formación

Sea L un alfabeto para una teoría de primer orden. Los axiomas en L pueden ser de tres tipos: axiomas lógicos, axiomas de reescritura y axiomas extralógicos.

Definición

El conjunto de axiomas lógicos es

$$Ax_{Log}(L) = Ax_1(L) \cup Ax_2(L) \cup Ax_3(L) \cup Ax_4(L) \cup Ax_5(L) \subset Fbf(L) \quad (1)$$

donde

$$\begin{aligned}
Ax_1(L) &= \{\phi \to (\psi \to \phi) | \phi, \psi \in Fbf(L)\} && (2)\\
Ax_2(L) &= \{(\phi \to (\psi \to \chi)) \to ((\phi \to \psi) \to (\phi \to \chi)) \,|\, \phi, \psi, \chi \in Fbf(L)\} && (3)\\
Ax_3(L) &= \{(\neg\phi \to \psi) \to ((\neg\phi \to \neg\psi) \to \phi) \,|\, \phi, \psi \in Fbf(L)\} && (4)\\
Ax_4(L) &= \{(\forall x\, \phi(x) \to \phi(\xi)) \,|\, \phi \in Fbf(L), \xi \in Term(L)\} && (5)\\
Ax_5(L) &= \{\forall x\, (\phi \to \psi(x)) \to (\phi \to \forall x\, \psi(x)) \,|\, \phi, \psi(x) \in Fbf(L)\} && (6)
\end{aligned}$$

Definición

El conjunto de axiomas de reescritura es

$$Ax_{RE}(L) = Ax_6(L) \cup Ax_7(L) \cup Ax_8(L) \cup Ax_9(L) \subset Fbf(L) \qquad (7)$$

donde

$$\begin{aligned}
Ax_6(L) &= \{(\psi \vee \phi) \leftrightarrow (\neg\phi \to \psi) | \phi, \psi \in Fbf(L)\} && (8)\\
Ax_7(L) &= \{(\psi \wedge \phi) \leftrightarrow \neg(\phi \to \neg\psi) | \phi, \psi \in Fbf(L)\} && (9)\\
Ax_8(L) &= \{(\psi \leftrightarrow \phi) \leftrightarrow \neg((\phi \to \neg\psi) \to \neg(\psi \to \phi)) | \phi, \psi \in Fbf(L)\} && (10)\\
Ax_9(L) &= \{(\exists x\, \phi(x)) \leftrightarrow \neg(\forall x\, \neg\phi(x)) | \phi, \psi \in Fbf(L)\} && (11)
\end{aligned}$$

Los axiomas extralógicos son propios de una teoría.

Campos algebraicos

Recordamos que un campo es una estructura algebraica $(A, +, \cdot, 0, 1)$ tal que

- la estructura aditiva $(A, +, 0)$ forma un grupo abeliano,
- el producto $\cdot$ se distribuye, por ambos lados, respecto a la adición, y
- la estructura multiplicativa de elementos no-nulos $(A - \{0\}, \cdot, 1)$ forma un grupo.

La noción de campo es formalizable en una teoría de primer orden.

Axiomas extralógicos en un alto nivel.

- Inclusión. "Un conjunto contiene a otro si todo elemento de ese otro está en el primero".
  $\forall a \forall b\, (\forall x\, (x \in a \rightarrow x \in b) \rightarrow a \subset b)$
- Extensionalidad. "Dos conjuntos coinciden si cada uno está incluído en el otro".
  $\forall a \forall b\, (a \subset b \ \wedge \ b \subset a \quad \leftrightarrow \quad a = b)$
- Apareamiento. "Dados dos conjuntos la pareja formada por ellos es un conjunto".
  $\forall a \forall b \exists c \forall x\, (x \in c \quad \leftrightarrow \quad x = a \ \vee \ x = b)$

- Esquema de separación. "Dado un conjunto y un predicado se puede formar el conjunto de elementos en el conjunto dado que satisfacen al predicado dado". Si $\phi(x,p) \in \mathrm{Fbf}(L_{TC})$ es una fórmula bien formada, el siguiente es un axioma:
  $\forall a \forall p \exists c \forall x \, (x \in c \quad \leftrightarrow \quad x \in a \ \wedge \ \phi(x,p))$
  En este caso se suele escribir $c = \{x \in a | \phi(x,p)\}$.
- Unión. "Dado un conjunto se puede formar la unión de todos sus elementos".
  $\forall a \exists b \forall x \, (x \in b \quad \leftrightarrow \quad \exists c \, (c \in a \ \wedge \ x \in c))$
  En este caso se suele escribir $b = \bigcup_{c \in a} c$.
- Conjunto de partes. "Dado un conjunto se puede formar el conjunto que consta de todos sus subconjuntos".
  $\forall a \exists b \forall x \, (x \in b \quad \leftrightarrow \quad x \subset a))$
  En este caso se suele escribir $b = \mathcal{P}(a)$.

- Infinito. Se dice que un conjunto a es inductivo si de las relaciones $c \in b$ y $b \in a$ se sigue que $c \in a$. El axioma del infinito asegura que: "Existe un conjunto inductivo que tiene al vacío como un elemento".
  $\exists i\ (\emptyset \in i\ \wedge\ \forall x\ (x \in i \quad \rightarrow \quad x \subset i))$
  Ya que en todo conjunto inductivo i se tiene que $\emptyset \in i$ y además, para cualquier x, si $x \in i$ entonces necesariamente $x + 1 := x \cup \{x\} \in i$, tenemos que todo conjunto inductivo es infinito, debido a lo cual se justifica el nombre del axioma. El más pequeño de los conjuntos inductivos se identifica con el conjunto $\mathbb{N}$ de los números naturales.
- Esquema de Reemplazo. Se dice que una fórmula bien formada $\phi(x, y, p) \in \mathrm{Fbf}(L_{TC})$ es funcional si "para cada x a lo sumo existe una sola y relacionada con x", es decir, si rige la implicación

$$\phi(x, y_1, p)\ \wedge\ \phi(x, y_2, p)\ \rightarrow\ y_1 = y_2$$

  El axioma de reemplazo asegura que: "La imagen de cualquier conjunto bajo un predicado funcional es un conjunto". Es decir, si $\phi(x, y, p) \in \mathrm{Fbf}(L_{TC})$ es funcional, entonces el siguiente es un axioma $\forall a\, \forall p\, \exists b \forall y\ \ (y \in b\ \leftrightarrow\ \exists x\ (x \in a\ \wedge\ \phi(x, y, p)))$.

- Regularidad. “Cualquier conjunto no-vacío posee un elemento minimal respecto a la relación de membresía”.
  $\forall a\,(\neg a = \emptyset \;\;\rightarrow\;\; \exists x\,(x \in a \;\wedge\; \forall y\;(y \in a \rightarrow \neg y \in x)))$
- Elección. “Cualquier familia no-vacía de conjuntos no-vacíos posee un producto cartesiano no-vacío”.
  $$\forall a\;(\neg a = \emptyset \;\wedge\; \forall y\;(y \in a \rightarrow \neg y \in \emptyset) \;\;\rightarrow$$
  $$\exists x\,\forall z\,(z \in a \;\rightarrow \exists y\;((z, y) \in x \;\wedge y \in z)))$$

Toda la teoría de conjuntos se desprende de estos axiomas.

Definición

$L = Sig \cup SL$ un alfabeto, $Sig = Cte \cup Fun \cup Rel$.

Interpretación para L, o *L-estructura*: $M \neq \emptyset$ y $\bar{\cdot}$ definida en Sig t.q.

1. Toda constante corresponde a un elemento en M:

$$\xi \in Cte \ \Rightarrow \ \overline{\xi} \in M$$

2. Toda función de aridad n corresponde a una $M^n \to M$:

$$f_j^n \in Fun \ \Rightarrow \ \overline{f_j^n} : M^n \to M$$

3. Toda relación de aridad n corresponde a un subconjunto en M^n:

$$R_j^n \in Rel \ \Rightarrow \ \overline{R_j^n} \subset M^n.$$

La pareja $\mathfrak{M} = (M, \bar{\cdot})$ es la interpretación o la L-estructura.

Definición

Sea $L = Sig \cup SL$ *un alfabeto para una teoría de primer orden, y sea* $\mathfrak{M} = (M, \bar{\cdot})$ *una interpretación. La interpretación de un término será bien un elemento de* M *o una función definida en alguna potencia cartesiana de* M*, según el término sea o no cerrado. Explícitamente, para cada término* ξ *en* L*, definimos su interpretación* $\overline{\xi}$ *de manera recursiva:*

1. *Si* $\xi = c$ *es una constante, entonces* $\overline{\xi} = \overline{c}$*:*

$$\xi = c \ , \ c \in Cte \ \Rightarrow \ \overline{\xi} = \overline{c}.$$

2. *Si* $\xi = x$ *es una variable, entonces* $\overline{\xi}$ *es la función identidad en* M*:*

$$\xi = x \ , \ x \in Var \ \Rightarrow \ \overline{\xi} : M \to M, m \mapsto m.$$

3. *Si* ξ *es un término compuesto, entonces* $\overline{\xi}$ *es la composición de las interpretaciones de sus componentes:*

$$\xi = f_j^n(\xi_1, \ldots, \xi_n) \ , \ f_j^n \in Fun \ \Rightarrow \ \overline{\xi} = \overline{f_j^n}(\overline{\xi_1}, \ldots, \overline{\xi_n}).$$

Definición

Sea $\mathfrak{M} = (M, \bar{\cdot})$ una interpretación de un alfabeto $L = Sig \cup SL$. Veamos ahora cómo se interpreta a los enunciados.

Enunciados atómicos. *Sea $R^i_j \in Rel$ un símbolo variable y sean $\xi_1, \ldots, \xi_i$ términos sin variables libres. Se dice que el átomo $R(\xi_1, \ldots, \xi_i)$ es* válido *en $\mathfrak{M}$, y se escribe $\mathfrak{M} \models R(\xi_1, \ldots, \xi_i)$, si $(\overline{\xi_1}, \ldots, \overline{\xi_i}) \in \overline{R}$.*

Enunciados negados. *Sea $\phi = \neg\psi$ un enunciado cuyo conectivo principal es la negación. Entonces definimos:*

$$\mathfrak{M} \models \phi \;:\Leftrightarrow\; \mathfrak{M} \not\models \psi.$$

Enunciados que son conjunciones. *Sea $\phi = \psi \wedge \chi$ un enunciado cuyo conectivo principal es la conjunción. Entonces definimos:*

$$\mathfrak{M} \models \phi \;:\Leftrightarrow\; (\mathfrak{M} \models \psi) \;\&\; (\mathfrak{M} \models \chi)\,.$$

Definición

Enunciados que son disyunciones. *Sea $\phi = \psi \vee \chi$ un enunciado cuyo conectivo principal es la disyunción. Entonces definimos:*

$$\mathfrak{M} \models \phi \ :\Leftrightarrow \ (\mathfrak{M} \models \psi) \ \textit{o} \ (\mathfrak{M} \models \chi) \, .$$

Enunciados que son implicaciones. *Sea $\phi = \psi \rightarrow \chi$ un enunciado cuyo conectivo principal es la implicación. Entonces definimos:*

$$\mathfrak{M} \models \phi \ :\Leftrightarrow \ [\, (\mathfrak{M} \models \psi) \ \Rightarrow \ (\mathfrak{M} \models \chi) \,] \, .$$

Enunciados que son equivalencias. *Sea $\phi = \psi \leftrightarrow \chi$ un enunciado cuyo conectivo principal es la equivalencia. Entonces definimos:*

$$\mathfrak{M} \models \phi \ :\Leftrightarrow \ [\, (\mathfrak{M} \models \psi) \ \Leftrightarrow \ (\mathfrak{M} \models \chi) \,] \, .$$

Definición

Enunciados cuantificados universalmente. *Sea $\phi = \forall x\, \psi(x)$ un enunciado, donde $\psi(x)$ es una fórmula en la que sólo la variable x aparece libre. Para cada término ξ en donde no aparezca x, denotemos por $\psi(x \leftarrow \xi)$ al enunciado que resulta de ψ al sustituir la variable x por ξ. Entonces definimos:*

$$\mathfrak{M} \models \phi \;\; :\Leftrightarrow \;\; \text{para cada término cerrado } \xi,\ \mathfrak{M} \models \psi(x \leftarrow \xi).$$

Enunciados cuantificados existencialmente. *Sea $\phi = \exists x\, \psi(x)$ un enunciado, donde $\psi(x)$ es una fórmula en la que sólo la variable x aparece libre. Entonces definimos:*

$$\mathfrak{M} \models \phi \;\; :\Leftrightarrow \;\; \text{para algún término cerrado } \xi,\ \mathfrak{M} \models \psi(x \leftarrow \xi).$$

Definición

Si Φ es un conjunto de enunciados en un alfabeto L y $\mathfrak{M}$ es una L-estructura, diremos que $\mathfrak{M}$ es un modelo de Φ, y escribiremos $\mathfrak{M} \models \Phi$, si toda fórmula en Φ es válida en $\mathfrak{M}$, i.e.

$$\phi \in \Phi \;\Rightarrow\; \mathfrak{M} \models \phi.$$

Así, por ejemplo, si $\mathrm{Ax}_{Log}(L)$ es la colección de axiomas lógicos y $\mathrm{Ax}_{RE}(L)$ la de axiomas de reescritura, entonces, según la observación precedente, cualquiera que sea la L-estructura $\mathfrak{M}$ se tiene $\mathfrak{M} \models \mathrm{Ax}_{Log}(L) \cup \mathrm{Ax}_{RE}(L)$.

Campos algebraicos: Números racionales

Sea $\mathbb{Z}^{2*} = \{(x, y)|x, y \in \mathbb{Z}, y \neq 0\}$ el conjunto de parejas de enteros cuyas segundas componentes no son cero. Si $(x, y) \in \mathbb{Z}^{2*}$, a la primera componente x se le llama numerador y a la segunda, y, denominador. En $\mathbb{Z}^{2*}$ se introduce la relación de equivalencia:

$$(x_1, y_1) \sim (x_2, y_2) \;\Leftrightarrow\; x_1 y_2 - x_2 y_1 = 0 \tag{12}$$

y al espacio cociente $\mathbb{Q} = \left(\mathbb{Z}^{2*}/\sim\right)$ se le llama el conjunto de números racionales. A cada elemento, que es en sí una clase de equivalencia, $[(x, y)]$ se le suele escribir $\frac{x}{y}$, o bien x/y. Evidentemente,

$$\begin{aligned} &\forall\, [(x, y)] \in \mathbb{Q}\, \exists x_1, y_1 \in \mathbb{Z} : \\ &(x, y) \sim (x_1, y_1) \;\&\; y_1 > 0 \;\&\; x_1, y_1 \text{ son primos relativos.} \end{aligned} \tag{13}$$

(evidentemente, si $r = \text{m.c.d.}(|x|, |y|)$ entonces hagamos $\sigma = 1$ si ambos x, y poseen el mismo signo, $\sigma = -1$ si x, y poseen signo distinto, $x_1 = \sigma\frac{|x|}{r}$ e $y_1 = \frac{|y|}{r}$.) La pareja $(x_1, y_1) = x_1/y_1$ se dice ser el representante reducido del racional $[(x, y)]$. En lo que sigue, representaremos a cada racional por su representante reducido.

Sea L_{CA} el alfabeto de la teoría de campos algebraicos. Se construye una interpretación $\mathfrak{Q} = (\mathbb{Q}, \bar{\cdot})$ como sigue:
Al símbolo 0 se le asocia el racional $\bar{0} = 0/1$.
Al símbolo 1 se le asocia el racional $\bar{1} = 1/1$.
A $+$ se le asocia la función

$$\bar{+} : ([x_1/y_1], [x_2/y_2]) \mapsto [(x_1 y_2 + x_2 y_1)/y_1 y_2].$$

A $\cdot$ se le asocia la función

$$\bar{\cdot} : ([x_1/y_1], [x_2/y_2]) \mapsto [x_1 x_2/y_1 y_2].$$

A $=$ se le asocia la relación de equivalencia $\sim$:

$$[x_1/y_1] = [x_2/y_2] \;\Leftrightarrow\; x_1 y_2 - x_2 y_1 = 0.$$

Puede verse que en $\mathfrak{Q}$ se satisfacen todos los axiomas de campos. Incluso más: este campo es conmutativo, es decir,

$$[x_1/y_1] + [x_2/y_2] = [x_2/y_2] + [x_1/y_1]$$

y es arquimediano, es decir,

$$\forall [x/y] \in \mathbb{Q}\, \exists n \in \mathbb{N} : \; [x/y] \leq n\bar{1}.$$

El conjunto de cuaterniones coincide con el espacio real de 4 dimensiones. Sea $Cuat = \mathbb{R}^4$. Si $x = (a, b, c, d) \in Cuat$ es un cuaternión, lo escribiremos como $x = a + bi + cj + dk$, y diremos que el cuaternión $\overline{x} = a - bi - cj - dk$ es su conjugado. Los números $1, i, j, k$ se dicen ser básicos

La suma de cuaterniones se define "entrada-a-entrada":

$$\begin{aligned} \left(a_1 + b_1 i + c_1 j + d_1 k\right) + \left(a_2 + b_2 i + c_2 j + d_2 k\right) &= \\ \left((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k\right) &. \end{aligned} \tag{14}$$

En cuanto al producto, definimos primeramente sobre los básicos las relaciones siguientes:

$$\begin{aligned} -1 &= i^2 = j^2 = k^2 \\ i &= jk = -kj \\ j &= ki = -ik \\ k &= ij = -ji \end{aligned}$$

Se tiene, naturalmente, que el inverso aditivo de cualquier cuaternión $x = a + bi + cj + dk$ es $-x = -a - bi - cj - dk$. Ahora, si $x \neq 0$ entonces al multiplicarlo por su conjugado, se obtiene:

$$x \cdot \overline{x} = a^2 + b^2 + c^2 + d^2 = \|x\|^2$$

así pues $x \cdot \frac{\overline{x}}{\|x\|^2} = 1$. En consecuencia, el inverso multiplicativo de x es, precisamente, $x^{-1} = \frac{\overline{x}}{\|x\|^2}$.

Cuat es entonces un campo y por ende una L_{CA}-estructura. con la interpretación construída como sigue:
Al símbolo 0 se le asocia el cuaternión $\overline{0} = (0, 0, 0, 0)$.
Al símbolo 1 se le asocia el cuaternión $\overline{1} = (1, 0, 0, 0)$.
A $+$ se le asocia la función suma definida por la ec. (14).
A $\cdot$ se le asocia la función producto definida por la ec. (15).
A $=$ se le asocia la relación de igualdad de $\mathbb{R}^4$:

$$(a_1, b_1, c_1, d_1) = (a_2, b_2, c_2, d_2) \;\Leftrightarrow\; \left\{ \begin{array}{l} (a_1 = a_2)\,\&\,(b_1 = b_2)\,\& \\ (c_1 = c_2)\,\&\,(d_1 = d_2) \end{array} \right.$$

Cuat es un campo que no es conmutativo, aunque sí es arquimediano.
Cuat contiene a los campos usuales de números reales y de números complejos: El campo de los números reales se identifica con el subconjunto $\mathbb{R}' = \{(a, 0, 0, 0) | a \in \mathbb{R}\}$ y el campo de los números complejos con el subconjunto $\mathbb{C}' = \{(a, b, 0, 0) | a, b \in \mathbb{R}\}$.

Teoría de conjuntos: Modelo estándar

Para construir este modelo, supondremos la existencia de los números ordinales. Recordamos que un ordinal es un conjunto transitivo, es decir, un conjunto x tal que

$$\forall y : \quad y \in x \;\Rightarrow\; y \subset x,$$

que además está bien ordenado bajo la relación $\in$, es decir, para cualquier subconjunto X de x existe un elemento $x_0 \in X$ tal que para todo $y \in X$ tal que $y \neq x$ se tiene $y \notin x_0$ (es decir, x_0 es un punto $\in$-minimal de X). Sea pues $Ord = \{x | x \text{ es un ordinal}\}$ la clase de números ordinales. Se tiene que para cualquier ordinal $x \in Ord$ se cumple sólo una de las siguientes tres aseveraciones:

1. x coincide con el conjunto vacío, es decir, x es el primer ordinal: $x = \emptyset$.
2. x es el sucesor de un ordinal: $\exists y \in Ord : \; x = y \cup \{y\}$.
3. x es un ordinal límite: $x = \bigcup_{y \in x} y$.

$\begin{array}{rcl} \mathbf{0} & = & \emptyset \\ \vdots & & \vdots \\ \mathbf{n}+\mathbf{1} & = & \mathbf{n} \cup \{\mathbf{n}\} \\ \vdots & & \vdots \end{array}$	$\begin{array}{lcl} \omega & = & \bigcup_{\mathbf{n}} \mathbf{n} \\ \vdots & & \vdots \\ \omega+\mathbf{n}+\mathbf{1} & = & (\omega+\mathbf{n}) \cup \{(\omega+\mathbf{n})\} \\ \vdots & & \vdots \end{array}$
$\begin{array}{lcl} \omega\cdot 2 & = & \bigcup_{\mathbf{n}} \omega+\mathbf{n} \\ \vdots & & \vdots \\ \omega\cdot 2+\mathbf{n}+\mathbf{1} & = & (\omega\cdot 2+\mathbf{n}) \cup \{(\omega\cdot 2+\mathbf{n})\} \\ \vdots & & \vdots \end{array}$	$\begin{array}{lcl} \omega\cdot(\mathbf{n}+\mathbf{1}) & = & \bigcup_{\mathbf{m}} \omega\cdot\mathbf{n}+\mathbf{m} \\ \vdots & & \vdots \\ \omega^2 & = & \bigcup_{\mathbf{n}} \omega\cdot\mathbf{n} \\ \vdots & & \vdots \end{array}$
$\begin{array}{lcl} \omega^{\mathbf{n}+1} & = & \bigcup_{\mathbf{m}} \omega^{\mathbf{n}}+\mathbf{m} \\ \vdots & & \vdots \\ \delta_2=\omega^{\omega} & = & \bigcup_{\mathbf{n}} \omega^{\mathbf{n}} \\ \vdots & & \vdots \end{array}$	$\begin{array}{lcl} \omega^{\omega^2} & = & \bigcup_{\mathbf{n}} \omega^{\omega\cdot\mathbf{n}} \\ \vdots & & \vdots \\ \delta_3=\omega^{\omega^{\omega}} & = & \bigcup_{\mathbf{n}} \omega^{\omega^{\mathbf{n}}} \\ \vdots & & \vdots \end{array}$
$\begin{array}{lcl} \vdots & & \vdots \\ \delta_{\mathbf{n}+1} & = & \omega^{\delta_{\mathbf{n}}} \\ \vdots & & \vdots \end{array}$	$\begin{array}{lcl} \vdots & & \vdots \\ \epsilon_0 & = & \bigcup_{\mathbf{n}} \delta_{\mathbf{n}} \\ \vdots & & \vdots \end{array}$

Definición

La jerarquía acumulativa de conjuntos *es la sucesión* $\mathcal{V} = (V_x)_{x \in Ord}$ *definida como sigue:*

$$\begin{aligned} V_0 &= \emptyset \\ V_{x+1} &= \mathcal{P}(V_x) \\ V_x &= \bigcup_{y \in x} V_y \text{ si } x \text{ es un ordinal límite.} \end{aligned}$$

Se tiene que $\mathcal{V}$ es una interpretación de todos los axiomas que determinan a la Teoría de Conjuntos de Zermelo-Fraenkel. Esta interpretación se llama estándar de la teoría de conjuntos.

De hecho, si denotamos por ω al primer ordinal límite, es decir, ω es el orden del conjunto de los números naturales, entonces V_ω es un conjunto de todos los axiomas de Zermelo-Fraenkel exceptuando al axioma de infinito. V_ω es pues un modelo donde todos los conjuntos son finitos.

Contenido

Deducción natural

Definición

En el cálculo de predicados se considera sólo dos reglas de inferencia:

Modus ponens *Para cualesquiera dos fórmulas ϕ, ψ:*

$$\frac{\begin{array}{l}\phi \rightarrow \psi \\ \phi\end{array}}{\psi} \tag{16}$$

Generalización *Para cualquier fórmula $\phi(x)$, donde x aparece libre en ϕ:*

$$\frac{\phi(x)}{\forall x\, \phi(x)} \tag{17}$$

Definición (Pruebas)

Sea $H \subset Fbf(L)$ una colección de fórmulas bien formadas sobre el lenguaje L, llamadas hipótesis. Una prueba es una sucesión finita $D = [\phi_1, \ldots, \phi_n]$ de fórmulas bien formadas tal que $\forall i \leq n$:

- $\phi_i \in$ *Axiomas, o*
- $\phi_i \in H$, *o*
- $\exists j, k < i : \ \phi_k = (\phi_j \rightarrow \phi_i)$
- $\exists j < i : \ \phi_k = \forall x \, \phi_j(x)$

En este caso la prueba D se dice ser una prueba de ϕ_n a partir de H. Se escribe $H \vdash \phi$ para denotar el hecho de que ϕ es demostrable, es decir, que existe una prueba de ϕ_n a partir de H.
El conjunto de fórmulas $Ded(H) = \{\phi \in Fbf(L) | H \vdash \phi\}$ consta de todas las fórmulas demostrables a partir de H. Éste se dice ser la teoría de H.

Proposición

Sean $H, \Phi, \Psi \subset Fbf(L)$ tres conjuntos de fórmulas y sean $\phi, \psi \in Fbf(L)$ otras dos fórmulas. Entonces vale la siguiente implicación:

$$\Phi \vdash \phi \ \& \ \Psi \cup \{\phi\} \vdash \psi \ \Rightarrow \ \Psi \cup \Phi \vdash \psi. \tag{18}$$

En consecuencia, el "operador" *Ded* es un operador de cerradura: Para cualesquiera $H_1, H_2 \subset \mathrm{Fbf}(L)$:

1. $H_1 \subset Ded(H_1)$.
2. $H_1 \subset H_2 \ \Rightarrow \ Ded(H_1) \subset Ded(H_2)$.
3. $Ded(Ded(H_1)) = Ded(H_1)$.

Definición

El conjunto de *teoremas* *en* L *es* $Ded(\emptyset)$, *es decir, es el conjunto de fórmulas demostrables partiendo únicamente de los axiomas. El conjunto de teoremas se dice ser también la* *teoría de primer orden* *resultante del lenguaje* L *con los Axiomas.*

Ejemplo

Para cada $\phi(x,y) \in Fbf(L)$ se tiene

$$\vdash (\forall x\, \forall y\, \phi(x,y)) \;\rightarrow\; (\forall y\, \forall x\, \phi(x,y))$$

es decir, cuantificadores universales consecutivos pueden intercambiarse.

1. $(\forall x\, \forall y\, \phi(x,y)) \;\rightarrow\; \forall y\, \phi(x,y)$ $\quad (Ax_4)$
2. $(\forall y\, \phi(x,y)) \;\rightarrow\; \phi(x,y)$ $\quad (Ax_4)$
3. $((\forall y\, \phi(x,y)) \;\rightarrow\; \phi(x,y)) \;\rightarrow$ $\quad (Ax_1)$
   $(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; ((\forall y\, \phi(x,y)) \;\rightarrow\; \phi(x,y)))$
4. $\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; ((\forall y\, \phi(x,y)) \;\rightarrow\; \phi(x,y))$ $\quad (MP\ 2,3)$
5. $(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; (\forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y))) \;\rightarrow$
   $((\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall y\, \phi(x,y)) \;\rightarrow\; (\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y)))$
   (Ax_2)

6. $(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall y\, \phi(x,y)) \;\rightarrow$
$(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y))$ *(MP 4, 5)*
7. $\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y)$ *(MP 1, 6)*
8. $\forall x\; (\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y))$ *(Gen 7)*
9. $\forall x\; (\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \phi(x,y)) \;\rightarrow$
$(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall x\, \phi(x,y))$ *(Ax_5)*
10. $\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall x\, \phi(x,y)$ *(MP 8, 9)*
11. $\forall y\; (\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall x\, \phi(x,y))$ *(Gen 10)*
12. $\forall y\; (\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall x\, \phi(x,y)) \;\rightarrow$ *(Ax_5)*
$(\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall y\, \forall x\, \phi(x,y))$
13. $\forall x\, \forall y\, \phi(x,y) \;\rightarrow\; \forall y\, \forall x\, \phi(x,y)$ *(MP 11, 12)*

Ejemplo

Para cada $\phi(x,y) \in Fbf(L)$ *se tiene*

$$\vdash \forall x \, \forall y \, (\phi(x,y) \rightarrow \neg\phi(y,x)) \rightarrow \forall x \, \neg\phi(x,x)$$

es decir, "un predicado que no es simétrico para ninguna pareja no puede cortar a la diagonal".

Escribiremos una prueba de ese teorema. Para simplificar la escritura mínimamente, abreviaremos

$$\Phi \equiv [\forall x \, \forall y \, (\phi(x,y) \rightarrow \neg\phi(y,x))] \,.$$

1. $\Phi \rightarrow \forall y \, (\phi(x,y) \rightarrow \neg\phi(y,x))$ (Ax_4)
2. $\forall y \, (\phi(x,y) \rightarrow \neg\phi(y,x)) \rightarrow (\phi(x,x) \rightarrow \neg\phi(x,x))$ (Ax_4)
3. $2. \rightarrow (\Phi \rightarrow 2.)$ (Ax_1)
4. $\Phi \rightarrow 2.$ $(MP\ 2,3)$

5. $(\Phi \to 2.) \to$ $((\Phi \to \forall y\ (\phi(x,y) \to \neg\phi(y,x))) \to$ $(\Phi \to (\phi(x,x) \to \neg\phi(x,x))))$ (Ax_2)

6. $(\Phi \to \forall y\ (\phi(x,y) \to \neg\phi(y,x))) \to$ $(\Phi \to (\phi(x,x) \to \neg\phi(x,x)))$ $(MP\ 4,5)$

7. $\Phi \to (\phi(x,x) \to \neg\phi(x,x))$ $(MP\ 1,6)$

8. $(\phi(x,x) \to \neg\phi(x,x)) \to$ $((\phi(x,x) \to \phi(x,x)) \to \neg\phi(x,x))$ (Ax_3)

9. $8. \to (\Phi \to 8.)$ (Ax_1)

10. $\Phi \to 8.$ $(MP\ 8,9)$

11. $(\Phi \to 8.) \to$ (Ax_2) $((\Phi \to (\phi(x,x) \to \neg\phi(x,x))) \to$ $(\Phi \to ((\phi(x,x) \to \phi(x,x)) \to \neg\phi(x,x))))$

12. $(\Phi \to (\phi(x,x) \to \neg\phi(x,x))) \to$ $(\Phi \to ((\phi(x,x) \to \phi(x,x)) \to \neg\phi(x,x)))$ $(MP\ 10,11)$

13. $\Phi \to ((\phi(x,x) \to \phi(x,x)) \to \neg\phi(x,x))$ $(MP\ 7,12)$

14. 13. $\rightarrow$
$(\Phi \rightarrow (\phi(x,x) \rightarrow \phi(x,x)) \rightarrow (\Phi \rightarrow \neg\phi(x,x)))$ (Ax_2)
15. $(\Phi \rightarrow (\phi(x,x) \rightarrow \phi(x,x))) \rightarrow (\Phi \rightarrow \neg\phi(x,x))$
$(MP\ 13, 14)$
16. $\phi(x,x) \rightarrow \phi(x,x)$ (Teo)
17. 16. $\rightarrow$ $(\Phi \rightarrow$ 16.$)$ (Ax_1)
18. $\Phi \rightarrow$ 16. $(MP\ 16, 17)$
19. $\Phi \rightarrow \neg\phi(x,x)$ $(MP\ 15, 18)$
20. $\forall x\ (\Phi \rightarrow \neg\phi(x,x))$ $(Gen\ 19)$
21. $\forall x\ (\Phi \rightarrow \neg\phi(x,x)) \rightarrow (\Phi \rightarrow \forall x\, \neg\phi(x,x))$ (Ax_5)
22. $\Phi \rightarrow \forall x\, \neg\phi(x,x)$ $(MP\ 20, 21)$

Definición

*Sea $P \subset Fbf(L)$ un conjunto de fórmulas bien formadas, $\phi_0 \in P$ una fórmula en P y sea $[\phi_1, \ldots, \phi_m]$ una prueba construída a partir de P. Se dice que ϕ_i **depende** de ϕ_0 si se cumple alguna de las proposiciones siguientes:*

1. $\phi_i = \phi_0$
2. ϕ_i *se sigue de alguna fórmula que depende de* ϕ_0.

Resulta claro que si ϕ_i no depende de ϕ_0, entonces vale la implicación:

$$P \cup \{\phi_0\} \vdash \phi_i \;\Rightarrow\; P \vdash \phi_i. \tag{19}$$

Teorema (de la Deducción)

Sea $P \subset Fbf(L)$ un conjunto de fórmulas bien formadas y sean $\phi_0, \phi \in Fbf(L)$ dos fórmulas. Supongamos que $P \cup \{\phi_0\} \vdash \phi$ y que existe una prueba de esto en la que la regla de generalización no se haya aplicado a ninguna fórmula que dependa de ϕ_0, respecto a una variable libre de ϕ_0. Entonces $P \vdash \phi_0 \to \phi$.

El recíproco del Teorema de Deducción,

$$P \vdash \phi_0 \to \phi \quad \Rightarrow \quad P \cup \{\phi_0\} \vdash \phi$$

es válido como una consecuencia de la regla Modus Ponens.

Proposición

Sea $\phi \in Fbf(L)$ una fórmula donde no aparezca libre la variable x y sea $\psi(x)$ una segunda fórmula con apariciones libres de x. Entonces en cualquier teoría T de primer orden:

$$T \vdash \phi \wedge \forall x\, \psi(x) \leftrightarrow \forall x\, (\phi \wedge \psi(x)) \tag{20}$$
$$T \vdash \phi \vee \exists x\, \psi(x) \leftrightarrow \exists x\, (\phi \vee \psi(x)) \tag{21}$$
$$T \vdash \phi \vee \forall x\, \psi(x) \leftrightarrow \forall x\, (\phi \vee \psi(x)) \tag{22}$$
$$T \vdash \phi \wedge \exists x\, \psi(x) \leftrightarrow \exists x\, (\phi \wedge \psi(x)) \tag{23}$$

En esta proposición es importante que x no aparezca libre en ϕ. Por ejemplo, en $\mathbb{R}$ para $x = -1$ la siguiente fórmula es válida:

$$(x+1) = 0 \;\wedge\; \forall x\, ((\exists y : x = y \cdot y) \rightarrow x \geq 0)$$

sin embargo es claramente falsa la fórmula

$$\forall x\, ((x+1) = 0 \;\wedge\; ((\exists y : x = y \cdot y) \rightarrow x \geq 0)).$$

Si $\mathcal{Q}$ es uno de los cuantificadores $\forall$ o $\exists$, sea $\mathcal{Q}'$ el otro cuantificador, es decir, el cuantificador tal que $\{\mathcal{Q},\mathcal{Q}'\} = \{\forall,\exists\}$.

Proposición

Sea $\phi \in Fbf(L)$ una fórmula donde no aparezca libre la variable x y sea $\psi(x)$ una segunda fórmula con apariciones libres de x. Entonces en cualquier teoría T de primer orden:

$$T \vdash (\phi \rightarrow \mathcal{Q}x\,\psi(x)) \leftrightarrow \mathcal{Q}x\,(\phi \rightarrow \psi(x)) \tag{24}$$

$$T \vdash (\mathcal{Q}x\,\psi(x) \rightarrow \phi) \leftrightarrow \mathcal{Q}'x\,(\psi(x) \rightarrow \phi) \tag{25}$$

Definición

Sea $\phi(x_1, \ldots, x_n) \in Fbf(L)$ una fórmula libre de cuantificadores (es decir, no contiene cuantificador alguno). Como en el cálculo proposicional, se dice que $\phi(x_1, \ldots, x_n)$ es una literal si es un átomo o la negación de un átomo. Una conjunción de literales es una frase y una disyunción de literales es una cláusula. Una forma conjuntiva es una conjunción de cláusulas y una forma disyuntiva es una disyunción de frases.

Proposición

Si $\phi(\mathbf{x}) \in Fbf(L)$ es una fórmula libre de cuantificadores, donde $\mathbf{x} = [x_1, \ldots, x_n]$ es la lista de sus variables, entonces se puede encontrar algorítmicamente sendas fórmulas $\psi(\mathbf{x}) =: FC(\phi(\mathbf{x}))$ en forma conjuntiva y $\chi(\mathbf{x}) =: FD(\phi(\mathbf{x}))$ en forma disyuntiva equivalentes ambas a $\phi(\mathbf{x})$.

Definición

Una fórmula $\phi(x_1, \ldots, x_n) \in Fbf(L)$ se dice estar en forma prenex si es de la forma

$$\phi(x_1, \ldots, x_n) \equiv \mathcal{Q}_1 y_1 \, \mathcal{Q}_2 y_2 \cdots \mathcal{Q}_m y_m \, \psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

donde cada $\mathcal{Q}_i$ es un cuantificador $\forall$ o $\exists$, y ψ es una fórmula libre de cuantificadores. Si además $\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ es una forma conjuntiva, entonces se dice que $\phi(x_1, \ldots, x_n)$ está en forma normal prenex.

Así en una forma prenex, los cuantificadores sólo aparecen al inicio de ella.

Proposición

Para toda fórmula $\phi(\mathbf{x}) \in Fbf(L)$, donde $\mathbf{x} = [x_1, \ldots, x_n]$ es la lista de sus variables libres, existe una fórmula $\psi(\mathbf{x}) \in Fbf(L)$ en forma normal prenex equivalente a ϕ. Más aún, ψ es algorítmicamente constructible a partir de ϕ.